190-1445

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN THE APPLICATION OF)
)
Michael George Bunn) Group Art Unit No.
)
SERIAL NO: To Be Assigned)
)
FILED: Herewith)
)
FOR: Printed Document Authentication)

#2

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents, Washington, D.C. 20231", on February 15, 2000.

Name of person signing Deborah E. Dudek

Signature Deborah E. Dudek

CLAIM FOR PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

Dear Sir:

Under the International Convention, for the purposes of priority, applicant claims the benefit of British Application No. 9906924.7, filed March 26, 1999.

A certified copy of said application is appended hereto.

DATE: February 15, 2000

Respectfully submitted,

William M. Lee

William M. Lee, Jr.
Registration No. 26,935

LEE, MANN, SMITH, MCWILLIAMS
SWEENEY & OHLSON
P.O. Box 2786
Chicago, Illinois 60690-2786
(312) 368-1300
Fax (312) 368-0034

The Patent Office

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

accordance with the rules, the words "public limited company" may be replaced by p.l.c., P.L.C. or PLC.

istration under the Companies Act does not constitute a new legal entity but merely s the company to certain additional company law rules.

Signed J Evans.

Dated 13 January 2000

CERTIFIED COPY OF
PRIORITY DOCUMENT

Patents Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

1/77

26MAR99 E435611-1 D02759
P01/7700 0.00 - 9906924.7

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference C1415

THE PATENT OFFICE
L
26 MAR 1999
RECEIVED BY POST

2. Patent application number
(The Patent Office will fill in this part) **9906924.7**

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

INTERNATIONAL COMPUTERS LIMITED
26 Finsbury Square, London EC2A 1DS

Patents ADP number *(if you know it)* 282 58 008

If the applicant is a corporate body, give the country/state of its incorporation ENGLAND

4. Title of the invention

PRINTED DOCUMENT AUTHENTICATION METHOD

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

D C Guyatt
Intellectual Property Department
International Computers Limited
Stevenage
Herts
SG1 2DY

Patents ADP number *(if you know it)* 1094 937 005

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	7
Claim(s)	1
Abstract	1
Drawing(s)	3 + 3 (8)

10. If you are also filing any of the following, state how many against each item.

Priority documents	—
Translations of priority documents	—
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	2
Request for preliminary examination and search *(Patents Form 9/77)*	—
Request for substantive examination *(Patents Form 10/77)*	—
Any other documents *(please specify)*	—

11. I/We request the grant of a patent on the basis of this application.

Signature D C Guyatt Date 24/3/99

12. Name and daytime telephone number of person to contact in the United Kingdom

D. C. Guyatt
01438 786235

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

C1415

PRINTED DOCUMENT AUTHENTICATION METHOD

Background to the Invention

This invention relates to a method for authenticating printed documents.

It is frequently required to provide some way of checking the authenticity of printed documents, to confirm that the document has been issued from a particular source, and that the information in it has not been tampered with. In particular, such authentication may be required for certificates of various kinds.

As an example, in the UK it is a requirement that any road vehicle over three years old should have a test certificate, referred to as an MOT certificate. These certificates are issued by licensed vehicle testing stations, following an inspection of the vehicle to check its roadworthiness and compliance with legal requirements. The certificate must be presented at a post office when the owner of the vehicle re-licenses it. Clearly, the post office should check that the certificate is not a forgery, and that the information in it has not been altered. At present, the post office clerk does this simply by making a cursory visual check.

The object of the invention is to provide an improved method for authenticating printed documents.

Summary of the Invention

According to the invention a method for authenticating a printed document comprises the following steps:

a) a document producer sends information to be included in a document to an authentication authority;
b) the authentication authority cryptographically generates an authentication code from this information, and sends the authentication code back to the document producer;
c) the document producer prints the document, including both the information and the authentication code; and
d) a document checker cryptographically checks the authentication code against the information in the document.

In the MOT certificate example described above, the document producer would be the vehicle testing station, the authentication authority may be a central agency run by (or with powers delegated by) the government Vehicle Inspectorate (VI), and the document checker may be the post office at which the MOT is presented.

The authentication code may be generated and checked using a secret key, which is known to both the authentication authority and the document checker. Alternatively, a public/private key pair may be used.

One document authentication method in accordance with the invention will now be described by way of example with reference to the accompanying drawings.

Brief Description of the Drawings

Figure 1 is a schematic diagram of a system for issuing and authenticating certificates.

Figure 2 is a flow chart showing the operation of a software component for issuing certificates.

Figure 3 is a schematic diagram showing a certificate produced by the system.

Description of an Embodiment of the Invention

Referring to Figure 1, the system involves the following entities:

- VI Data Centre 101. This is a central agency, run by the Vehicle Inspectorate (VI).
- Vehicle testing stations (VTS) 102. These are authorised by the VI to test vehicles and to issue MOT certificates. Each vehicle testing station may employ one or more authorised vehicle testers to carry out the tests.
- Post Offices 103.

The VI Data Centre includes a central server computer 104, and a database 105. The database holds details of all licensed vehicles, vehicle testing stations, and authorised vehicle testers. The VI Data Centre has a secret key, referred to below as the VI secret key.

Each of the vehicle testing stations 102 has a computer terminal 106, which can communicate with the central server 104 by way of a network 107. The terminal is connected to a printer 108, which is used for printing the MOT test certificates 109. The printer 108 incorporates a barcode scanner, so that it can read barcodes on blank certificates inserted into the printer.

Each of the terminals 106 includes communications software, which manages communications between terminal and the central server. All communications between terminal and the central server are encrypted, to ensure that messages cannot be intercepted. In addition, security technology is used to verify the authenticity of both ends of the link, to prevent a rogue device from linking into the network and pretending to be a terminal.

In operation, a vehicle tester can enter information relating to a particular vehicle test into the terminal. The terminal includes a function which allows the vehicle tester to confirm the results of a test and, if the results are confirmed, to print a test certificate or failure notice as appropriate. Figure 2 shows this function in more detail.

(Step 201) The function first displays the test information, with the overall result (pass or fail) summarised.

(Step 202) The function then asks the tester to confirm whether or not the test results are correct. If they are not correct, the function exits, and the tester may then go back to change the test information.

(Step 203) If the tester confirms that the results are correct, the function then branches according to the test result.

(Step 204) If the test result was "pass", the function prompts the user to specify whether the test certificate is to be printed locally, at the test station, or mailed directly from the VI Data Centre to the registered keeper of the vehicle.

(Step 205) If the test certificate is to be printed locally, the function prompts the user to feed a blank pass certificate into the printer 108. Each blank pass certificate has a unique pre-printed serial number, and a barcode containing the serial number, as well as other security features such as a watermark. The VI keeps a record of the serial numbers of the certificates issued to each testing station, so that each certificate can be traced back to a particular testing station.

(Steps 206-207) When the certificate is in the printer, the function instructs the barcode scanner incorporated in the printer to scan in the certificate serial number. The terminal

then transmits a message to the central server. The message contains details of the tester and the test station, the certificate serial number, the vehicle details, and the test results.

When the central server 104 receives this message, it performs a final check to confirm that the tester and the vehicle test station are duly authorised to perform the test.

Assuming this check is satisfactory, the central server proceeds as follows. First, it generates a message authentication code (MAC) from a predetermined sub-set of information in the message. In this example, the MAC is generated by performing a key-dependent one-way hash of the information, using the VI secret key. The central server transmits this MAC back to the terminal.

(Step 208) When the terminal receives the MAC, it prints the certificate. The contents of the certificate are described below.

(Step 209) If on the other hand the test certificate is to be mailed directly to the registered keeper of the vehicle, the function transmits the test information to the central server, with a request for a mailed certificate. The central server performs checks as described above, and if these checks are satisfactory, prints the certificate.

(Steps 210 - 212) If the test result was "failure", the function prompts the user to feed a blank failure notice into the printer. The function then transmits the test information to the central server, and prints the failure notice.

Figure 3 shows the format of the certificate. It includes the following:

- Certificate number 301
- Test date 302
- Expiry date of certificate 303.
- Vehicle details 304.
- MAC 305, as a string of characters.
- Bar code 306. This represents the MAC in bar code form.

Referring again to Figure 1, each of the Post Offices 103 is provided with at least one terminal 112, having a bar code reader 113. It is assumed that the terminal has knowledge of the VI secret key.

When a vehicle owner presents an MOT certificate at the post office, the post office clerk uses the bar code reader 113 to scan the bar code 306 on the certificate, so as read the MAC into the terminal.

The clerk also types in the predetermined sub-set of information from the certificate (i.e. the same sub-set as used by the central server to generate the MAC). The terminal then uses this information, along with the VI secret key, to generate a MAC, and compares this with the MAC read from the bar code. If they are not equal, the terminal generates a message to alert the clerk.

If for any reason the bar code reader will not read the bar code, the clerk may type the MAC into the terminal, from the printed version of the VI signature. Alternatively, the terminal may display the MAC it has generated, so that the clerk can visually compare this with the MAC printed on the certificate.

In summary, it can be seen that the system described above allows a certificate to be authenticated quickly and easily.

Some possible modifications

It will be appreciated that many modifications may be made to the system described above without departing from the scope of the present invention. For example, instead of using a secret key to form the MAC and to check it, a public/private key pair may be used.

Instead of requiring the clerk to type information from the certificate into the terminal, the information could be scanned in.

The vehicle test station could be arranged to authenticate the previous year's certificate, before generating a new one.

It should be noted that the invention is not restricted to issuing of MOT certificates as described above, but can be used in any application where it is required to authenticate a printed document.

CLAIMS

1. A method for authenticating a printed document comprising the following steps:

a) a document producer sends information to be included in a document to an authentication authority;

b) the authentication authority cryptographically generates an authentication code from this information, and sends the authentication code back to the document producer;

c) the document producer prints the document, including both the information and the authentication code; and

d) a document checker cryptographically checks the authentication code against the information in the document.

2. A method according to claim 1 wherein the document producer includes a bar code in the document, containing the authentication code, and wherein the document authenticator is provided with means for reading the bar code to obtain the authentication code.

3. A method for authenticating a printed document, substantially as hereinbefore described with reference to the accompanying drawings.

4. Apparatus for authenticating a printed document, substantially as hereinbefore described with reference to the accompanying drawings.

ABSTRACT

A method for authenticating a printed document is described. A document producer sends information to be included in a document to an authentication authority. The authentication authority cryptographically generates an authentication code from this information, and sends the authentication code back to the document producer. The document producer then prints the document, including both the information and the authentication code, and a bar code representing the authentication code. A document checker scans in the bar code, and cryptographically checks the authentication code against the information in the document.

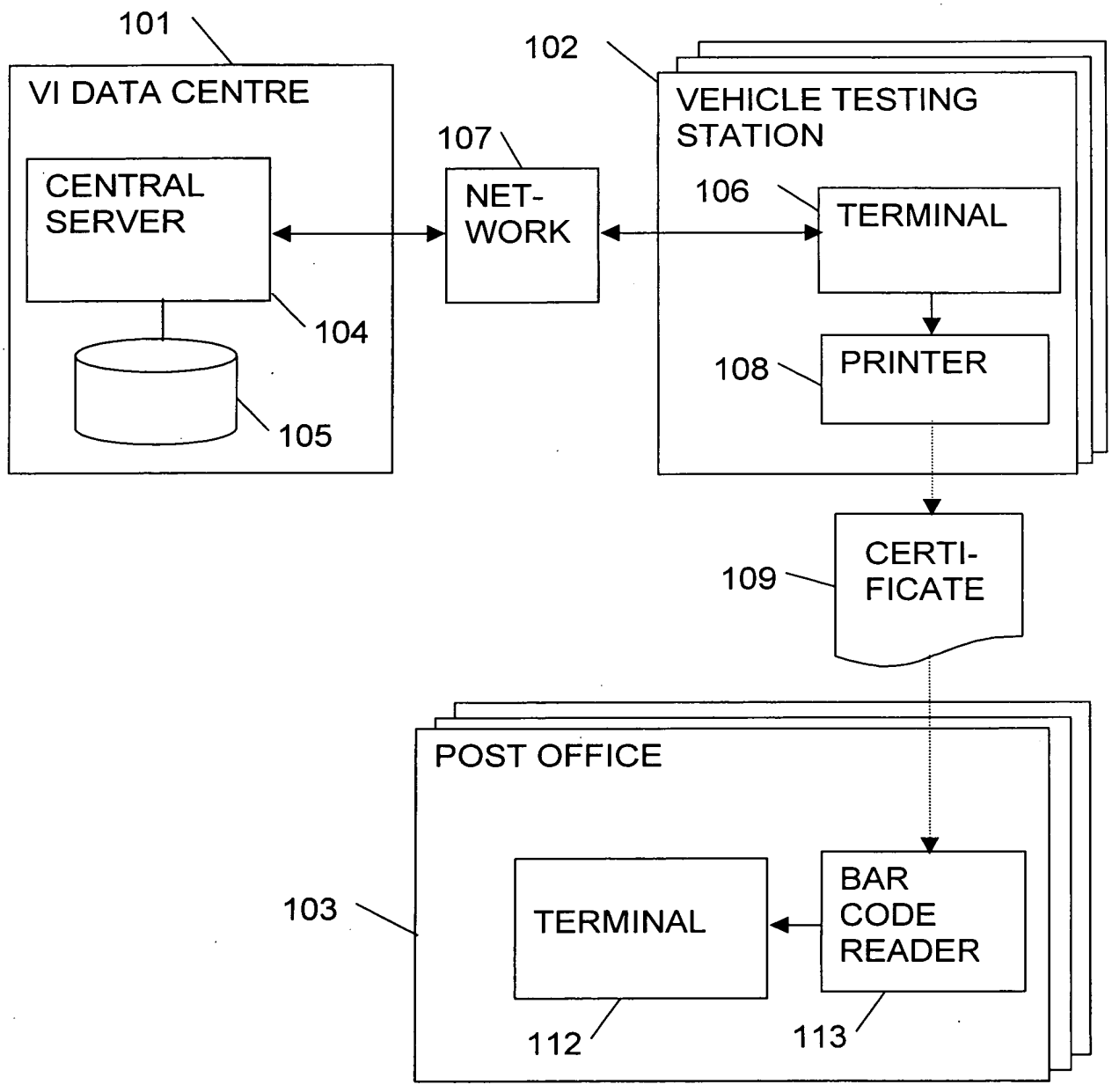
101
VI DATA CENTRE
CENTRAL SERVER
104
105
107
NET-WORK
102
VEHICLE TESTING STATION
106
TERMINAL
108
PRINTER
109
CERTI-FICATE
POST OFFICE
103
TERMINAL
112
BAR CODE READER
113

FIG.1

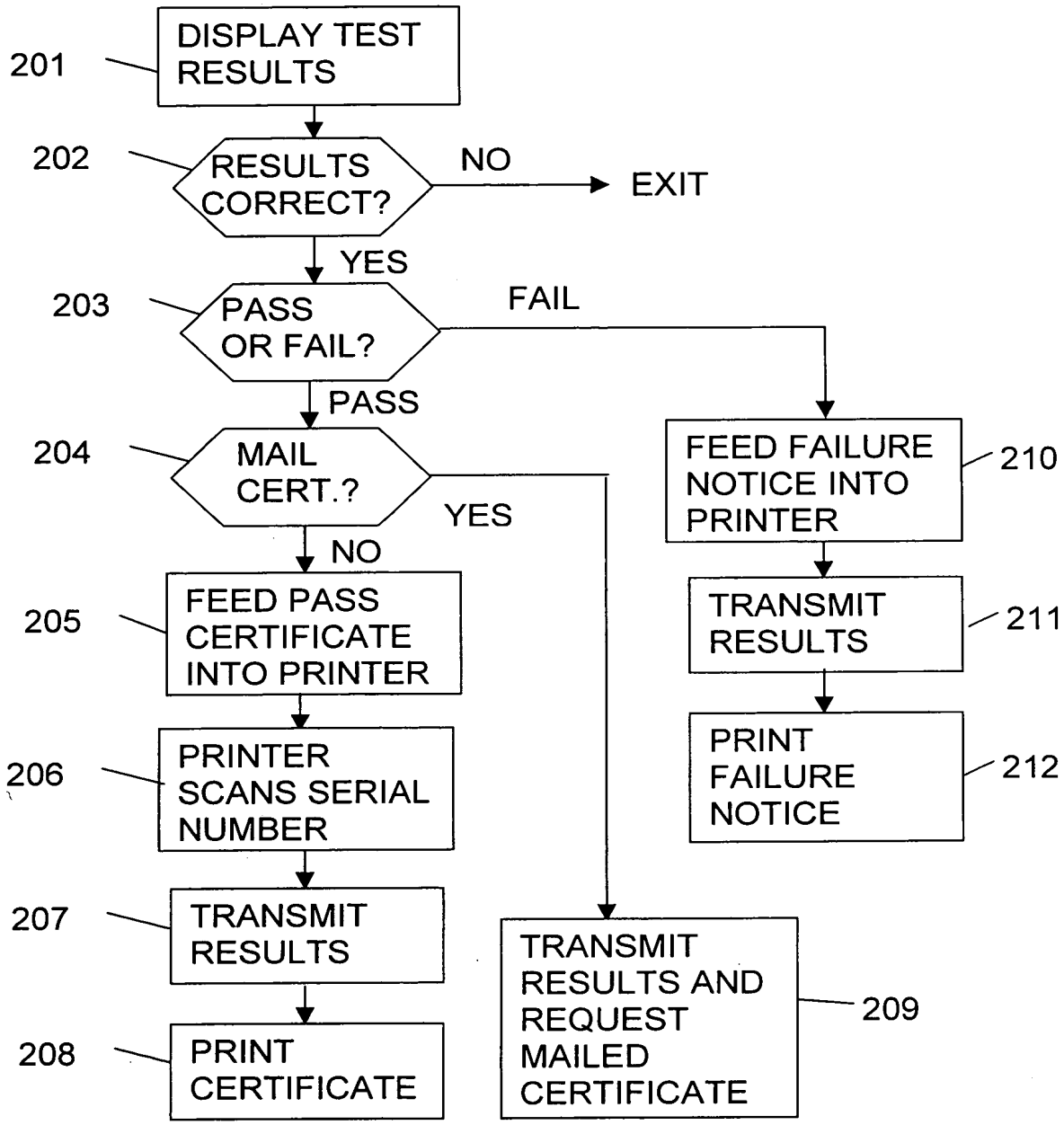
201
DISPLAY TEST RESULTS
202
RESULTS CORRECT?
NO
EXIT
YES
203
PASS OR FAIL?
FAIL
PASS
204
MAIL CERT.?
YES
NO
205
FEED PASS CERTIFICATE INTO PRINTER
206
PRINTER SCANS SERIAL NUMBER
207
TRANSMIT RESULTS
208
PRINT CERTIFICATE
209
TRANSMIT RESULTS AND REQUEST MAILED CERTIFICATE
210
FEED FAILURE NOTICE INTO PRINTER
211
TRANSMIT RESULTS
212
PRINT FAILURE NOTICE

FIG.2

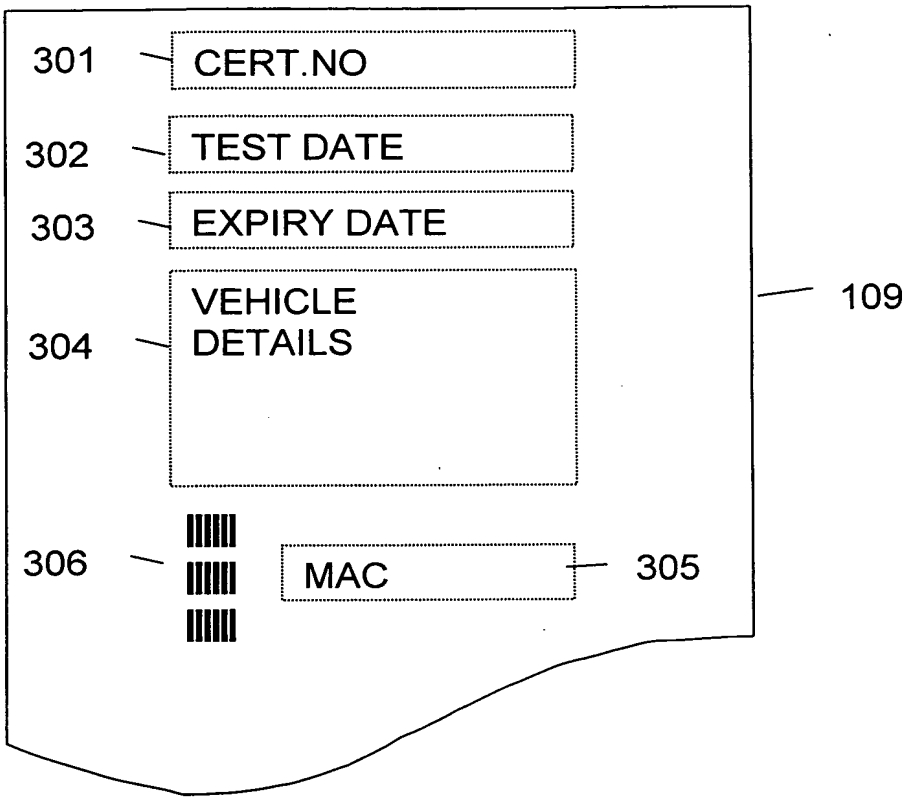
301
CERT.NO
302
TEST DATE
303
EXPIRY DATE
304
VEHICLE
DETAILS
306
MAC
305
109

FIG. 3